IN THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Previously Presented) A communications router for use in a communications network including a plurality of routers controlled by one or more trusted parties and at least one network control computer communicating with said communications router, said communications router comprising:

a transceiver to transmit and receive messages;

an electronic memory circuit having network information stored therein; and

an electronic processor circuit which (i) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning router of the plurality of routers and is to be excised from the network; (ii) determines an authenticity of the excising signal; (iii) excises the first router when the excising signal is authenticated; and (iv) reroutes the excising signal to at least a second router of the plurality of routers when the excising signal is authenticated.

2. (Original) A communications router according to Claim 1, wherein said electronic processor circuit excises the first router by (a) adding the first router to information regarding routers stored in said electronic memory circuit, (b) removing from said electronic memory circuit routing updates corresponding to the first router, (c) removing the first router from a neighbor table stored in said electronic memory circuit when the first router is listed therein, and (d) recomputing a forwarding table to direct future routing.

3. (Previously Presented) A communications router according to Claim 2, wherein said electronic processor circuit further causes a message to be transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic.

4. (Original) A communications router according to Claim 3, wherein said electronic processor circuit further: (i) evaluates a signal received through the transceiver from another network router; (ii) identifies which network router the signal has been received from; (iii) determines if the network router is listed with the information regarding excised routers; (iv) discards the signal when the router is listed; and (v) processes the signal when the router is not listed.

5. (Original) A communications router according to Claim 1, wherein said electronic processor circuit determines the authenticity of the excising signal using a public encryption key.

6. (Previously Presented) A communications router according to Claim 1, wherein said electronic processor reinstates the first router when said communications router receives and verifies a reinstate message from the network control computer.

7. (Previously Presented) In a communications system for communications among a plurality of routers controlled by one or more trusted parties in a network, at least one network control computer being linked to a first router of the plurality of routers, each of the communications routers including a transceiver to transmit and receive messages, a method of operating the first router comprising the steps of:

evaluating an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a second functioning router of the plurality of routers and is to be excised from the network;

determining an authenticity of the excising signal;

excising the second router when the excising signal is authentic; and

rerouting the excising signal to at least a third router of the plurality of routers.

8. (Original) A method according to Claim 7, wherein said excising step comprises (a) adding the second router to information regarding routers stored in a memory, (b) removing from the communications router routing updates corresponding to the second router, (c) removing the second router from a neighbor table of the communications router when the second router is listed therein, and (d) recomputing a forwarding table.

9. (Original) A method according to Claim 8, further comprising steps of transmitting a message to the network control computer and disregarding the excising signal when the excising signal is not authentic.

10. (Original) A method according to Claim 8, further comprising the steps of:

evaluating a signal received through the transceiver from another network router;

identifying which network router a signal has just been received from;

determining if the network router is identified by the information regarding excised routers;

discarding the signal when the router is listed; and processing the signal when the router is not listed.

11. (Original) A method according to Claim 7, further comprising the steps of:

evaluating a signal received through the transceiver from another network router;

identifying which network router the signal has just been received from;

determining if the network router is identified by information regarding non-compromised routers stored in a memory;

discarding the signal when the router is not listed; and

processing the signal when the router is listed.

12. (Previously Presented) A method according to Claim 7, wherein said excising step comprises (a) removing the second router from information stored in a memory regarding routers controlled by trusted parties, (b) removing from the communications router routing updates corresponding to the second router, (c) removing the second router from a neighbor table of the communications router when the second router is listed therein, and (d) recomputing a forwarding table.

13. (Original) A method according to Claim 12, further comprising steps of transmitting a message to the network control computer, and disregarding the excising signal when the excising signal is not authenticated.

14. (Original) A method according to Claim 7, wherein the excising signal is authenticated using a public encryption key.

15. (Original) A communications router according to Claim 7, further comprising the step of reinstating the second station when the communications router receives and verifies a reinstate message from the network control computer.

16. (Previously Presented) A mobile communications station which communicates among a plurality of mobile stations controlled by a first of parties in an ad-hoc network in which stations are arranged in clusters of communication member stations, with one member station in each cluster being a head station for the cluster, each member station communicating with the network through at least one cluster head station, a cluster head station communicating with zero or more cluster head stations, a network computer being linked with said mobile communications station, said mobile communications station comprising:

a transceiver which transmits signals to and receives signals from other mobile stations in the network,

a memory having network information stored thereon; and

a processor which (i) operates said mobile communications station as a cluster head or cluster member station; (ii) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning cluster head or cluster member station and is to be excised from the network; (iii) verifies the authenticity of the excising signal; (iv) excises the first cluster head or cluster member station when the excising signal is authentic; and (v) distributes the excising signal to at least a second cluster head or cluster member station.

17. (Previously Presented) In a communications system for communications in a network among a plurality of wireless routers controlled by one or more trusted parties, at least one control computer being linked to a first router of the plurality of wireless routers, each of the wireless routers including a transceiver to transmit and receive messages, a method of operating the network comprising the steps of:

formulating in the control computer an excise signal indicating that an untrusted party has gained control of at least a second functioning router and is to be excised from the network, providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router;

verifying the signature on the excise signal in the first router, and when the signature is valid (a) adding the information identifying the second router to information regarding excised routers stored in memory of the first router, (b) removing from the first router routing updates corresponding to the second router, (c) removing information corresponding to the second router from a neighbor table of the first router when the second router is listed therein, and (d) recomputing a forwarding table in the first router;

redistributing the excise signal to each of the plurality of routers, except for the second router; and

upon receiving a message from another one of the plurality of routers, determining, in each of the plurality of routers, , an identifier for the router from which the message is received and processing the message only when the information regarding excised routers does not include the identifier.

18. (Original) The method according to Claim 17, further comprising steps of transmitting a message to the control computer from the first router and causing the first router to disregard the excise signal each when the excise signal is not authentic.

19. (Original) A method according to Claim 18, wherein the digital signature is validated using a public encryption key.

20. (Original) A method according to Claim 19, further comprising the step of reinstating the excised second router.

21. (Original) A method according to Claim 20, wherein a router disregards the message when the information regarding excised routers includes the identifier.

22. (Previously Presented) In a communications system for communications in a network among a plurality of wireless routers controlled by one or more trusted parties, at least one control computer being linked to a first router of the plurality of routers, each of the routers including a transceiver to transmit and receive messages, a method of operating the network comprising the steps of:

formulating in the control computer an excise signal indicating that at least a second functioning router is controlled by an untrusted party and is to be excised from the network, providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router;

verifying the signature on the excise signal in the first router, and when the signature is valid removing the information identifying the second router from information stored in memory of the first router regarding routers controlled by trusted parties ;

redistributing the excise signal to each of the plurality of routers, except for the second router; and

determining, in each of the plurality of routers when receiving a message from another one of the plurality of routers, an identifier for the router from which the message is received from and processing the message only when the information regarding routers controlled by trusted parties includes the identifier.

23. (Original) The method according to Claim 22, further comprising steps of transmitting a message to the control computer from the first router and causing the first router to disregard the excise signal each when the excise signal is not authentic.

24. (Previously Presented) A communications router for use in a communications network, the network including a plurality of routers controlled by one or more trusted parties, at least one network control computer communicating with said communications router, said communications router comprising:

a transceiver to transmit and receive messages,:

means for storing network information;

means for evaluating an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that a first functioning router of the plurality of routers is controlled by an untrusted party and is to be excised from the network;

means for authenticating the excising signal;

means for excising the first router when the excising signal is authentic; and

means for rerouting the excising signal to at least a second router of the plurality of routers.

25. (Previously Presented) In a communications system for communications among a plurality of routers in a network controlled by one or more trusted parties, at least one computer being linked to a first router of the plurality of routers, a method of operating the network comprising the steps of:

authenticating in the first router a cut-off signal received from the control computer, the cut-off signal indicating that the control computer has determined that at least one functioning router is controlled by an untrusted party and is to be cut-off from communicating with the network;

preventing the first router from communicating with the at least one cut-off router when the signal is authenticated;

redistributing the cut-off signal to each of the plurality of routers, except for the at least one cut-off router, and preventing each of the remaining routers from communicating with the at least one cut-off router,

wherein when a router receives a message from one of the plurality of routers, the router determines if the message is from the at least one cut-off router, and processes the message only when the message is not from the at least one cut-off router.

26. (Previously Presented) In a communications system for communication among a plurality of routers in a network controlled by one or more trusted parties, at least one computer being linked to a first router of the plurality of routers, a method of operating the network comprising the steps of:

authenticating in the first router a cut-off signal received from the control computer, the signal indicating that the control computer has determined that at least one functioning router is controlled by an untrusted party and is to be cut-off from communicating with the network;

preventing the first router from communicating with the at least one cut-off router when the signal is authenticated;

redistributing the cut-off signal to each of the plurality of routers, except for the at least one cut-off router, and preventing each of the remaining routers from communicating with the at least one cut-off router,

wherein when a router receives a message from one of the plurality of routers, the router determines if the message is from a router other than the at least one cut-off router, and processes the message only when the message is from a router other than the at least one cut-off router.

27. (Previously Presented) In a communications system for communications among a plurality of routers controlled by a set of trusted parties in a network having verifiable information identifying at least one functioning router which has become controlled by an untrusted party, a method of operating the network comprising the steps of:

excising the identified router from the network ; and

determining whether messages transmitted between the plurality of routers are from the identifiedrouter.

28. (Previously Presented) The method according to Claim 27, further comprising a step of reinstating the identified router when a trusted party regains control of the router.

29. (Previously Presented) The method according to Claim 27, wherein the plurality of routers are prevented from communicating with the identified router.

30. (Previously Presented) The method according to Claim 29, wherein said determining step comprises consulting a data structure representing excised routers to determine if the router is controlled by an untrusted party.

31. (Previously Presented) The method according to Claim 29, wherein said determining step comprises consulting a data structure representing trusted routers to determine if the router is controlled by a trusted party.

32. (Previously Presented) Computer executable code stored on a computer readable medium, the code to operate a communications router in a network having a plurality of routers controlled by one or more trusted parties, at least one computer being linked to the communications router, each of the plurality of routers including a transceiver to transmit and receive messages, said computer executable code comprising:

code to excise from the network a functioning router that has become controlled by an untrusted party;

code to verify that messages transmitted among the plurality of routers are from routers controlled by trusted parties; and

code to reinstate an excised router when it a trusted party regains control of the excised router.

33. (Previously Presented) In a communications system for communications among a plurality of routers controlled by one or more trusted parties in a network, each of the routers maintaining information regarding functioning routers in the network that have become controlled by untrusted parties, a method of operating a network router comprising the steps of:

receiving a message from one of the plurality of routers in the network;

determining a router identifier for the router that just transmitted the message;

determining whether the information regarding functioning routers in the network that have become controlled by an untrusted party includes the router identifier; and

disregarding the message when the router is listed in the information regarding routers controlled by an untrusted party.

34. (Currently Amended) In a communications system for communications among a plurality of routers controlled by one or more trusted parties in a network, each of the routers maintaining information regarding routers in the network controlled by the trusted parties, a method of operating a network router comprising the steps of:

receiving a message from one of the plurality of routers in the network;

determining a router identifier for the router that just transmitted the message;

determining whether the information regarding routers controlled by trusted parties in the network includes the router identifier; and

when the router is not listed in the information regarding routers controlled by trusted parties, determining that the router is a functioning router that ~~has become compromised~~ is controlled by an untrusted party and disregarding the message.

35. (Previously Presented) A method of excising a router controlled by an untrusted party from an ad-hoc network, the network including a plurality of routers controlled by one or more trusted parties, at least one network control computer communicates with at least one of the plurality of routers, said method comprising the steps of:

determining that a functioning router of the plurality of routers in the network has become controlled by an untrusted party;

excising the router controlled by the untrusted party from the network; and

preventing the plurality of routers from communicating with the router controlled by the untrusted party.

36. (Previously Presented) The method according to Claim 35, wherein said determining step comprises determining a router is controlled by an untrusted party through embedded firewall functionality provided in each of the plurality of routers.